A

Live Traffic Analysis of TCP/IP Gateways

Phillip A. Porras
porras@csl.sri.com
Computer Science Laboratory

SRI International
333 Ravenswood Avenue
Menlo Park, CA 94025

Alfonso Valdes
avaldes@csl.sri.com
Electromagnetic and Remote Sensing Laboratory
SRI International
333 Ravenswood Avenue
Menlo Park, CA 94025

The work presented in this paper is currently funded by DARPA/ITO under contract number F30602-96-C-0294.

Point of Contact: Phillip A. Porras
Phone: (415) 859-3232
Fax: (415) 859-2844

August 1 1997

ABSTRACT

We enumerate a variety of ways to extend both statistical and signature-based intrusion-detection analysis techniques to monitor network traffic. Specifically, we present techniques to analyze TCP/IP packet streams that flow through network gateways for signs of malicious activity, nonmalicious failures, and other exceptional events. The intent is to justify, by example, the expense (in computational resources and human oversight) of introducing network surveillance mechanisms to monitor network traffic. We present this discussion of gateway surveillance modules as complementary to the filtering mechanisms of a large enterprise network, and illustrate their utility in directly enhancing the security and stability of network operations.

1. Introduction

Significant progress has been made toward the development of mechanisms to parse and filter hostile external network traffic, and thus prevent it from entering internal network environments [Firewalls94,Chapman95]. Mechanisms for preventing such traffic from reaching internal network services have become widely accepted as prerequisites for limiting the exposure of internal network assets, while providing interconnectivity with external networks. The encoding of filtering rules for packet or transport-layer communication should be enforced at key entry points between internal networks and external traffic. Developing filtering rules that strike an optimal balance between the restrictiveness necessary to suppress the entry of unwanted traffic, while allowing the necessary flows demanded for user functionality, can be a nontrivial exercise.

In addition to intelligent filtering, there have also been various developments in recent years in passive surveillance mechanisms to monitor network traffic for signs of malicious or anomalous (e.g., potentially erroneous) activity. Such tools attempt to provide network administrators timely insight into noteworthy exceptional activity. Realtime monitoring promises an added dimension of control and insight into the flow of traffic between the internal network and its external environment. The insight gained through fielded network traffic monitors could also aid sites in enhancing the effectiveness of their firewall filtering rules.

However, traffic monitoring is not a free activity---especially live traffic monitoring. Our discussion of network analysis techniques are presented fully realizing the costs they imply with respect to computational resources and human oversight. For example, obtaining the necessary input for surveillance involves the deployment of instrumentation to parse, filter, and format, event streams derived from potentially high-volume packet transmissions. Complex event analysis, response, and management of the units also introduce cost. Clearly, the introduction of network surveillance components on top of already deployed protective traffic filters is an expense that requires justification. In this paper, we outline the benefits of our techniques and seek to persuade the reader that these costs can be worthwhile.

[This paper will appear in the Proceedings of the
1998 Symposium on Network and Distributed System Security.
A final version will appear on this web page by November 1997.
Please check back then if you would like a copy. Thank you]

short.html